FILE Legal 3

EO 12065

OGC 81-03477
28 April 1981

MEMORANDUM FOR: Director, National Foreign Assessment Center
Deputy Director for Operations
Deputy Director for Science & Technology
Deputy Director for Administration
Comptroller
Legislative Counsel
Director of Personnel Policy, Planning, and Management
Director of Public Affairs
Director, Equal Employment Opportunity
Director of Security
Special Assistant to the DCI for Compartmentation
Director of Information Services, DDA

FROM : Daniel B. Silver
General Counsel

SUBJECT : Revised Draft of E.O. 12065

1. A revised draft of proposed changes to E.O. 12065 is enclosed for your review. This draft incorporates recommended revisions suggested by both components within the Agency, and the other member agencies of the interagency working group examining this order. The enclosed draft includes a section-by-section analysis of the proposed changes, with a statement of each individual proposal, the agency or agencies suggesting the change in parentheses, a discussion of the need for the recommended revision, and amended language where appropriate.

2. The interagency working group will be meeting tentatively this Friday, 1 May 1981, at 2:00 to discuss these proposed changes. The enclosed document is still at the draft stage, so that further comments concerning additional revisions are still welcomed. Any comments concerning the draft should be communicated orally to [redacted] of my office. STAT

STAT [redacted]

Enclosure

81-0602/2

Section-by-Section Analysis

Preamble.

Proposal: The order's primary purpose should be the protection of national security information, which should be emphasized in an amended preamble to the order. (CIA).

Discussion: The preamble to present E.O. 12065 states that order's purpose to be the balancing of "the public's interest in access to government information with the need to protect certain national security information from disclosure." The tone of the preamble is reflected throughout the order, that is, that in balancing these two interests the public's need to know is generally to be accommodated even if release of the information at issue could cause damage to the national security. As amended, the preamble would reflect a more appropriate balance between the need to adequately protect national security information from unauthorized disclosure and ensuring necessary public access to such information.

> Suggested Revision: Preamble. It is vital that certain information in the Government's possession be uniformly protected against unauthorized disclosure. It also essential that the public be informed concerning the activities of its government. The interests of the United States and its citizens require that certain information which is essential to our national defense and security be given only limited dissemination. To ensure that such information is adequately safeguarded, this order identifies the information to be so protected, prescribes classification, declassification, and safeguarding procedures to be followed, and establishes a monitoring system to ensure its effectiveness.

Section 1. Original Classification.

Subsection 1-1. Classification Designation.

i. Proposal: Paragraph 1-101's present provision establishing the order as the exclusive basis for classification unnecessarily impairs the use of protections provided national security information by other statutes and should be deleted. Paragraph 1-101 should include instead a provision similar to the one contained in Section 2 of former E.O. 10501, stating that the order in no way intends to limit the provisions of other statutes which afford additional protection to national security information. (CIA, NSA).

Discussion: Paragraph 1-101 of the order states that, with the exception of the Atomic Energy Act of 1954, E.O. 12065 provides the only basis for classifying information. Previous orders 11652 and 10501 did not specifically address whether they constituted the exclusive authority for classification, and did not expressly limit or affect the protection afforded by other statutes such as 50 U.S.C. §403 (d)(3) (intelligence sources and methods) or 18 U.S.C §798 (cryptologic information). Section 2 of E.O. 10501 specifically provided that "[n]othing in this order shall be construed to authorize the dissemination, handling or transmission of classified information contrary to the provisions of any statute." A similar provision should be included in the revised order to ensure that the protections afforded national security information by other statues are not inadvertently or unnecessarily limited by the issuance of this order.

ii. Proposal: The "less restrictive" presumption contained in paragraph 1-101 should be deleted and a positive provision provided on the need to adequately safeguard information whose classification level or classifiability is in doubt. (CIA, NSA).

Discussion: Paragraph 1-101 presently limits classification designations to one of three categories (Top Secret, Secret, and Confidential), and directs that any doubts concerning the appropriate classification level or whether information is classifiable at all should be resolved by using the less restrictive category or not classifying the information. This provision should be amended to provide that such information is to be classified at the higher level or is to remain classified until a determination is made as to the appropriate level of or the need for classification.

> Suggested Revision: 1-101. Information or material that requires protection against unauthorized disclosure in the interest of national security shall be classified in one of the three categories listed below. Information and material should be protected at an appropriate level of classification until a final determination is made as to the need for protection and the level of required protection. No other categories of classification shall be used to identify information or material as requiring protection in the interest of national security, except as otherwise provided by statute. Nothing in this Order shall be construed as limiting the protection afforded national security information by other provisions of law.

iii. Proposal: The "identifiable" harm standard provided in the definition of "Confidential" contained in paragraph 1-104 should be deleted and replaced by E.O. 11652's "cause damage" standard. (CIA, NSA).

Discussion: Paragraph 1-104 presently provides that information may be classified as "Confidential" when its unauthorized disclosure could reasonably be expected to cause at least identifiable damage to the national security. This "Confidential" classification designation is tied to paragraph 1-302, which requires a specific finding of "identifiable" damage prior to classification. Former E.O. 11652 permitted classification at the Confidential level when disclosure could be expected to "cause damage" to the national security, and did not require any separate finding of identifiable damage prior to classification. While E.O. 12065 does not make any provision as to what constitutes "identifiable" harm, it clearly is an obvious departure from the looser "cause damage" standard of E.O. 11652. Certain courts have viewed this "identifiable harm" standard as requiring agencies to fully detail the specific harm-in-fact which would result from disclosure of the information. This excessively expansive view of "identifiable" has caused considerable difficulty, compelling agencies in many cases to make the secret virtually a matter of public record in order to successfully defend the classification decision. The need to demonstrate such "identifiable" harm should be eliminated. Section 1-302's requirement that a separate finding concerning identifiable damage be made prior to classification should also be amended to conform with this revised "cause damage" standard. While deletion of this "identifiable" harm standard will not eliminate the requirement that officials fully justify classification decisions by being able to clearly articulate the

likely consequences of unauthorized disclosure, it should lessen the risk of classified information being compromised through satisfaction of an often impractical and unnecessarily fact-specific burden of proof.

Suggested Revision: 1-104. "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

Subsection 1-2. Classification Authority.

i. Proposal: The present limitation on the agencies provided classification authority should be reconsidered to ease burdensome classification processing in certain cases. (State, NSA).

Discussion: Paragraphs 1-201 through 203 expressly limit the number of agencies provided authority to make original classifications of information and set forth the level of classification authority which each agency is permitted to exercise. E.O. 12065 stripped eleven agencies of classification authority altogether, and provided reduced authority to five other agencies. This removal of classification authority has burdened certain departments (i.e., State; Defense), which must now classify documents for agencies (i.e., FDA, EPA; NSA) which create and receive classified information on a fairly regular basis but have no classification authority of their own. Restoration or provision of appropriate classification authority should be provided for agencies with a demonstrable need to exercise such authority on a continuing basis. Submissions by individual agencies concerning their need for classification authority should be requested and considered in revising this

section of the order.

ii. Proposal: Section 1-204(a) should be amended to permit officials designated by an agency head to determine which agency employees should be provided with Top Secret classification authority. (State, NSA, CIA).

Discussion: E.O. 11652 provided no limitation on the delegation of classification authority, except that such delegation be in writing. In order to limit the number of persons with classification authority, Section 1-204 of E.O. 12065 presently provides that only those agency heads listed in Section 1-201 may determine which employees should be given Top Secret classification authority. An agency head's inability to delegate this responsibility to other officials should be corrected given the other demands made of such officials' time and energies. Section 1-204 also limits delegation of Top Secret classification authority to officials who have "a frequent need to exercise such authority." The word "frequent" should be deleted in order to permit delegations to officials who exercise such authority on a continuing or recurring though not necessarily regular basis. The word "original" should also be inserted in the title of Section 1-204 to make clear that these limitations on delegation apply to original rather than derivative classification.

Suggested Revision: 1-204. Limitations on Delegation of Original Classification Authority.

Authority for original classification of information as Top Secret may be delegated

only to principal subordinate officials who have a need to exercise such authority as determined by the President, by agency heads listed in Section 1-201, or by a senior official with Top Secret classification authority who is granted this responsibility in writing by an agency head listed in Section 1-201.

Subsection 1-3. Classification Requirements.

i. Proposal: Three additional categories of classifiable information concerning cryptography, information whose disclosure could place an individual's life in jeopardy and information relating to the protective mission of the United States Secret Service should be added to paragraph 1-301, and use of that paragraph's catchall category should be facilitated by increasing the number of persons who may make determinations thereunder and deleting the requirement that such determinations be reported to the Information Security Oversight Office ("ISOO"). (State, Treasury, NSA, CIA).

Discussion: The present Executive Order limits classification by setting out seven specifically enumerated categories of classified information and providing that a document may not be classified unless it falls within one of these categories. §1-103(a)-(g). While the old order did not contain categories into which information must be fitted, it did provide specific examples of "top secret" and "secret" information. E.O. 11652, §1 (A)-(B).

The categories provided by the present Executive Order (i.e., intelligence activities, sources and methods, foreign relations-activities of the United States, scientific-economic

matters relating to national security), are sufficiently broad in most cases so as not to present any significant obstacle to classification. By providing specific categories of information, the order also provides officials with some discernible guidelines in making these classification decisions, and thus renders such decisions less susceptible to challenge as arbitrary and capricious. Several types of sensitive information, however, have been difficult to fit within this protective scheme and may thus require specific inclusion as new categories of classifiable information. One such category concerns information whose disclosure would place an individual's life in jeopardy. While E.O. 11652 specifically exempted such material from its declassification requirements, the present E.O makes no provision for this type of information. The State Department has found that "the absence of specific authority makes it difficult to protect information which would lead to physical harm, perhaps even death, to individuals who are not sources of information but may be referred to in documents, e.g., persons in Viet Nam or Iran who may be mentioned as friendly to the U.S."

NSA has also had some difficulty in FOIA and other litigation in fitting cryptographic and communication security matters within the "intelligence activities, sources, and methods" category. Providing specific authority for information pertaining to cryptography should facilitate the protection of this information.

Similarly, the Secret Service has encountered problems in justifying the classification of information relating to the techniques and procedures utilized in its protective mission. These protective techniques and procedures and other related information clearly impact on the national security, particularly when used in connection with the protection of the President or visiting foreign heads, dignitaries and officials, and should thus be provided greater protection by inclusion within Section 1-3 of a specific category of information covering such material.

In this regard, the seventh elastic category of information should also be amended to permit classification of other similar types of information which do not readily fit within any of the listed categories. Section 1-301(g) presently permits "other categories of information which are related to national security" to be classified, but requires determinations under this section to be made by the President, officials designated by the President, or agency heads. This category's availability for use should be expanded to permit all original classification authorities to classify information under its provisions. Additionally, paragraph 1-304, which requires all determinations made under this category to be reported promptly to the Director of the ISOO, should be deleted. This reporting requirement inhibits the legitimate use of this seventh category by suggesting that such determinations are inherently questionable and subject to review and oversight by a party outside of the particular agency.

A rewording of the initial sentence of paragraph 1-301 would also be helpful in this regard. Rather than characterizing this provision as an absolute bar to classification, the section's introduction instead should emphasize that it provides positive authority for classifying information that falls within the listed categories.

Suggested Revision: 1-301. Information may be considered for classification if it concerns:

(a) military plans, weapons, or operations;

(b) foreign government information;

(c) intelligence activities, sources or methods;

(d) foreign relations or foreign activities of the United States;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) cryptography or communications security matters;

(h) an individual whose life or safety may be placed in immediate jeopardy by disclosure of such information;

(i) techniques, procedures or material relating to the protective mission of the United States Secret Service; or

(j) other categories of information which are related to national security and which require protection against unauthorized disclosure.

ii. Proposal: In addition to broadening the categories of information for which specific authority for classification is provided, a new paragraph 1-302 */ should be added which would recognize the "aggregate" or "mosaic" effect in this classification process.

Discussion: This "aggregate" effect provision would authorize the classification of information whose disclosure in isolation might not be harmful to the national security, but whose disclosure in conjunction with the release of other information may result in such damage. While it is desirable to require officials to articulate with reasonable specificity the likely consequences of disclosure, particularly in terms of later defending such decisions, it is often impossible as a practical matter to weigh such damage in isolation without viewing the context in which this information will be released. In order to facilitate excerpting and other uses, some type of marking or labelling could be utilized, where practicable, to place the user on notice that the classification of this information is conditioned on the release of other related material.

> Suggested Revision: 1-302. Even though information is determined to concern one or more of the criteria in Section 1-301, it may not be classified unless an original classification authority also determines that its unauthorized disclosure reasonably could be

---

*/ As noted above, present paragraph 1-302 which requires a separate finding of identifiable damage prior to classification should be amended to conform with the lessened standard of harm required to classify information at the "Confidential" level.

> expected to cause damage to the national security. In considering whether the disclosure of information could be expected to cause damage to the national security, it is not necessary to consider such information in isolation. Information may be classified if its unauthorized disclosure in conjunction with one or more other actual or potential disclosures, reasonably could be expected to cause such damage.

iii. Proposal: The present presumption contained in Section 1-303, which provides that "unauthorized disclosure of foreign government information or the identity of a confidential foreign source is presumed to cause at least identifiable damage to the national security," should be expanded so as to apply to all confidential sources and to other sensitive intelligence information relating to the internal functioning or operations of intelligence agencies. The additional protection afforded foreign government information by present ISOO regulations should also be included in the order and should be extended to all of the above information. (State, CIA).

Discussion: First, the protection presently afforded "foreign confidential sources" should be expanded to apply to all "confidential sources." The present perceived inability of agencies to adequately protect the identity of confidential sources is not limited to foreign sources. If individuals are to be encouraged to provide their Government with confidential information, they must be able to repose some measure of confidence in the ability of that Government to protect the confidentiality of their relationship and the information so provided. Second, paragraph 1-303's presumption should also be

extended to information concerning the internal functioning and operations of intelligence agencies. If intelligence agencies are to effectively operate, their personnel, methods of operations, and internal workings must be afforded greater protection. Third, the protection afforded foreign government and confidential source information should also be strengthened by directly incorporating into the EO some of the additional safeguards presently provided by ISOO regulation at 32 C.F.R. §2002.5(b). Fourth, to conform with the lessened standard of damage justifying classification, "identifiable" should be deleted from Paragraph 1-303.

> Suggested Revision: 1-303. Unauthorized disclosure of foreign government information, information which could compromise the identity of a confidential source or information relating to intelligence methods, or the organization, function, names, official titles, salaries, or number of personnel employed by U.S. Government intelligence elements, is presumed to cause damage to the national security.
>
> The unofficial publication, in the United States or abroad, of the above described information contained in United States or foreign documents, or of substantially similar information, does not in or of itself constitute or justify the declassification of such documents. Although prior unofficial publication may affect determinations as to continuation of classification, there may be valid reasons for continued protection of the information which could preclude its declassification. In particular, the classification status of foreign government or confidential source information which concerns or derives from intelligence activities, sources or methods shall not be affected by any unofficial publication of identical or similar information.

iv. As noted above, paragraph 1-304, which requires all classification determinations made pursuant to paragraph 1-301(g)'s "catchall" category to be reported to ISOO, should be deleted. (NSA, CIA)

1-4. Duration of Classification.

i. Proposal: Paragraph 1-402's requirement that only individuals with Top Secret classification authority may extend classification beyond six years should be amended to permit the extension of classification by any official who is authorized to classifiy that level of information. The requirement that extension of this six-year declassification date be exercised "sparingly" should also be deleted, and a uniform time period of thirty years should be established for the mandatory declassification review of all national security information. (CIA, FBI, NSA, DOJ, State).

Discussion: Subsection 1-4 presently provides that information is to be automatically declassified after 6 years unless an official with Top Secret classification authority extends classification beyond this period. This extension authority is "to be used sparingly," and a declassification review must be undertaken, in any event, within thirty years after original classification for foreign government information and within twenty years for all other classified information. The admonition that this authority to extend classification beyond six years be used "sparingly" should be deleted. As with many of the other negative authorizations contained in E.O.

12065, the ability to classify information beyond artifically imposed time periods should not be inhibited if required in the interest of national security. Secondly, the date for mandatory declassification review should be uniformly set at thirty years for all information. Thirty years is a more realistic time frame in which to review intelligence information, particularly information received from or concerning sources who, in many cases, are still actively involved or subject to compromise by the release of such information. Moreover, such uniformity would also simplify administration of the order by eliminating the need for page-by-page review of documents in order to segregate foreign government information from other information because of the different review requirements applicable to each type of information. Lastly, the present limitation on the individuals who may extend classification beyond six years to officials with Top Secret classification authority should be removed. This restriction has resulted in unnecessary delays and duplication in agency review procedures. Instead, any official with authority to classify a designated category of information should also be able to extend that information's classification beyond six years.

Suggested Revision: 1-402. The classification of information may be extended for more than six years from the date of the original classification by an official who is authorized to make original classification determinations with respect to information of that classification designation. In such cases, a declassification date or event, or a date for review, shall be set. This date or event shall be as early as national security permits and shall be no more than thirty years after original classification.

1.5. Identification and Markings.

i. Proposal: Paragraph 1-501(a)'s requirement that the identity of the classifier be noted should be deleted and replaced by the method of identification utilized in E.O. 11652 of simply providing the title of the highest individual authorizing classification. Additionally, the classification warnings presently placed on paper copies should be required on all other forms of classified material to the extent practicable. Such markings would not be required, however, when their inclusion on documents or other material could compromise or impair intelligence operations or personnel. (CIA, NSA).

Discussion: Paragraph 1-501(a) requires that paper copies of all classified documents contain the identity of the original classification authority. This section, in conjunction with paragraph 2-102 concerning derivative classification, has required the adoption of complex number designator and derivative classification schemes in order to protect the identity of individual officials, and has led to considerable confusion and allegations by both the GAO and the courts that agencies have failed to satisfy these various marking requirements in certain instances. The use of number identifiers and names of original classification authorities has also caused Privacy Act problems by subjecting otherwise exempt data files to the requirement of that Act. E.O. 11652 simply provided that the title of the individual at the highest level authorizing classification should be identified, unless the individual who signed the document is

also the classifier, in which case no further annotation is required. Identification of the title of the highest authority authorizing classification would adequately serve the order's intent of encouraging responsible and thoughtful classification determinations, while simplifying the multiple classification marking schemes in use at present. Secondly, paragraph 1-501 should be amended to provide that the classification warnings presently required on paper documents should be prominently displayed, where practicable, on all types of classified information regardless of its physical form or medium. Notifying individuals that they are handling classified material and are expected to observe certain safeguards in using and further disseminating such material should be encouraged to the extent that placement of such classification warnings is practicable. Finally, paragraphs 1-501 and 4-102 should be amended to permit the omission of classification markings when the markings themselves would disclose a covert relationship not otherwise evident from the document's contents. Certain documentation required in establishing cover and other operational arrangements, while containing classified information, may not be so marked without compromising the bearer or recipient of such documentation. In these circumstances, a waiver of the marking requirements should be available.

> Suggested Revision: 1-501. At the time of original classification, the following should be shown on the face of paper copies of all classified documents, and prominently displayed, where practicable, on all other forms of classified information, except where such

markings would reveal a confidential source or relationship not otherwise evident from the face of such documents or information:

(a) the highest authority authorizing the classification, unless the individual who signs or otherwise authenticates a document or item has also authorized the classification, in which case no further annotation as to his identity is required;

(b) the office of origin;

(c) the date or event for declassification or review; and

(d) one of the three classification designations defined in Section 1-1.

ii. Proposal: Paragraph 1-502's requirement that documents whose classification is extended beyond six years must be marked with the identity of the individual who authorized the prolonged classification should be deleted. (State, NSA).

Discussion: This is an unnecessarily burdensome requirement that does not appear to serve any useful purpose. Paragraph 1-502's further requirement that the reason for the prolonged classification be stated ensures that such extensions will be carefully reviewed and justified, and removes the need for imposing additional identifier marking requirements.

Suggested Revision: 1-502. Documents classified for more than six years shall be annotated with the reason the classification is expected to remain necessary, under the requirements of Section 1-3, despite the passage of time. The reason for the prolonged classification may be stated by reference to criteria set forth in agency implementing regulations. These criteria shall explain in narrative form the reason the information needs to be protected beyond six years.

iii. Proposal: Section 1-504 should be amended to permit agency heads listed in paragraphs 1-201 and 1-202, to grant portion-marking waivers "for good cause" for all classes of documents or information. (State, CIA).

Discussion: Paragraph 1-504 provides that each classified document must clearly indicate which portions are classified or unclassified, and the level of classification of those portions which are classified. The Director of ISOO is authorized to grant exemptions for good cause from this portion marking requirement for specific classes of documents or information. Portion-marking is frequently time-consuming, difficult to enforce, and in the case of certain types of information (i.e., contractor generated documents, raw or semi-processed intelligence information), impractical or prohibitively costly to implement. Portion-marking also increases, in many cases, the possibility of compromising classified information by: (a) encouraging the fragmentation of documents not intended for such fragmentation; (b) compounding the problem of erroneous classification in bibliographic and other citations; (c) unnecessarily highlighting information from sensitive sources; and (d) increasing the likelihood of inadvertent clerical and transmission errors. Agency heads shouuld be authorized to grant portion-marking waivers for any class of documents when a showing of "good cause" is made. "Good cause" in these circumstances would include any of the above reasons (i.e., time or cost

burdens, increased likelihood of compromising information, impracticability) as determined by the appropriate agency heads.

Suggested Revision: 1-504. In order to facilitate excerpting and other uses, each classified document shall, by marking or other means, indicate clearly which portions are classified, with the applicable classification designation, and which protions are not classified. Agency heads listed in paragraphs 1-201 and 1-202 may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information.

Section 1-6. Prohibitions.

i. Proposal: Paragraph 1-601 should more clearly reflect the principle that classification may be used only to protect national security information and not to conceal violations of law and other proscribed activities.

Discussion: Paragraph 1-601 provides that classification may not be used to "conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition." While the intent of this provision is desirable, and should be retained, the current language is ambiguous and gives rise to an unintended inference that information whose disclosure would damage the national security must nonetheless be disclosed if it also includes information of the type specified above. Classification should be based solely on national security considerations, and should be prohibited only when undertaken for the purpose of concealing violations of law, inefficiency, or embarrassment to individuals.

Suggested Revision: 1-601. Classification shall be determined solely on the basis of national security considerations. In no case shall information be classified in order to conceal violations of law, inefficiency or administrative error, to prevent embarrassment to a person, or organization or agency, or to restrain competition, or to prevent for any other reason the release of information which does not require protection in the interest of national security.

ii. Proposal: Paragraph 1-602 should be deleted. (NSA).

Discussion: Paragraph 1-602 provides that "basic scientific research information not clearly related to the national security may not be classified." This provision is troublesome in that it provides a possible basis for challenging the classification of scientific research conducted in connection with national security activities in the event that such research is used in or has some application to non-national security related activities. Paragraph 1-605 already clearly states that "classification may not be used to limit dissemination of information that is not classifiable under the provisions of this Order." Additionally, paragraph 1-604 provides that documents which simply refer to classified information, without disclosing or containing such information themselves, may not be classified. These provisions adequately ensure that research which is only marginally related to the national security will not be classified on this basis alone, and makes deletion of paragraph 1-602 appropriate given its availability as a basis for challenging scientific research classification determinations.

iii. Proposal: Paragraph 1-603 should be deleted since its provision has undercut the protections provided by the Patent

Secrecy Act, and has otherwise impaired government efforts to protect sensitive technological information originating in the private sector but impacting significantly on the country's national security. (Treasury, CIA).

Discussion: Paragraph 1-603 provides that a product of non-government research or development may not be classified unless the government acquires a proprietary interest in the product. This section is not intended to affect the provisions of the Patent Secrecy Act (5 U.S.C. §§181-88). The Patent Secrecy Act specifically permits the Patent Office to order that an invention be kept secret and to withhold the grant of a patent if disclosure of an individual's invention is determined by certain designated defense agencies to be detrimental to the national security. This ability to deny patent applications for national security purposes is provided with regard to inventions in which the government has no proprietary interest. The Act also authorizes the issuance of Secrecy Orders by the Patent Office in such cases, which strictly limit access to and disclosure of information contained in these patent applications. The practical significance of not permitting the government to classify information relating to products in which it has no proprietary interest, but authorizing the issuance of secrecy orders which limit access and disclosure in the same fashion, is not readily apparent. More importantly, government efforts to limit dissemination of information that may be vital to technological developments contained in national defense applications has been undermined by this ambiguous provision.

iv. Proposal: Paragraph 1-606 should be retained and its authorization to classify documents after a FOIA request has been received should be reinforced, while reducing at the same time the administrative burdens entailed in this classification process. (State, Treasury, DOJ, CIA, NSA).

Discussion: Paragraph 1-606 of the present EO restricts the use of classification after a document has been requested under the FOIA or the non-statutory "Mandatory Review" process. Only senior agency officials with Top Secret classification authority are authorized to classify documents originated before the effective date of the order upon receiving a FOIA request. Documents originated on or after the effective date of E.O. 12065, may be classified after an agency has received a FOIA or mandatory review request only by the agency head or deputy agency head. This provision should be amended to permit agency heads to delegate this classification authority for documents originated after the effective date of the order to senior officials below the deputy agency head level. Given the number of FOIA requests that agencies receive, and the inevitability that errors and oversights will occur in the classification process, officials below the deputy agency head level should be authorized to make such decisions in order to relieve the administrative burden imposed on agencies by this

unnecessary restriction. While there has been some suggestion that this provision be deleted altogether, this ignores the benefit this provision provides in authorizing the classification of information after a request for its release has been received by an agency. This authorization should be strengthened rather than deleted, by rewording this provision to affirmatively permit such classification.

> Suggested Revision: 1-606. A document may be classified [upon or after receipt of a FOIA or Mandatory Review] request...if such classification... is authorized by the agency head or by a senior official granted such authority in writing by the agency head. Classification authority under this provision shall be exercised on a document-by-document basis.

v. Proposal: Paragraph 1-607 should be amended to permit classification to be restored to documents which are inadvertently released to the public when further damage to the national security can be prevented by retrieving the document and limiting further public dissemination. (State, Treasury, NSA, FBI).

Discussion: Paragraph 1-607 provides that classification may not be restored to documents already declassified and released to the public. The word "official" should be inserted before the word "released" to make clear that leaks and other unauthorized disclosures of information to the public do not serve to automatically declassify that information. As to information which is officially released to the public, but is done so inadvertently or by mistake, the order should permit continued classification of such information when the document

can be recovered and public exposure minimized. Former Department of Defense ("DOD") directives implementing E.O. 11652 permitted the reclassification of documents which could be recovered and further public dissemination of which could be reasonably minimized. These two conditions on restoring classification in cases of inadvertent release are important, because to the extent that the documents cannot be recovered or public exposure significantly minimized, then the harm the prevention of which justifies classification will already have occurred.

> Suggested Revision: 1-607. Classification may be restored to documents already declassified and officially released to the public under this Order or prior Orders only if authorized by a Top Secret classification authority who has determined that the previous declassification decision was erroneous, and that further damage to the national security may be prevented by recovery of the document and limiting additional public dissemination.

vi. Proposal: A new paragraph 1-608 should be added to the revised order to ensure continued protection for classified information provided to the Judicial Branch in connection with litigation or related matters. (NSA).

Discussion: Language similar to that found in Section 8 of the Classified Information Procedures Act, P.L. 96-456, which authorizes the continued classification of information introduced into evidence under protective conditions in court proceedings, should be included in the revised order. This provision would remove any ambiguity as to the continued classifiability of such information.

Suggested Revision: 1-608. Classified information and materials provided to courts in connection with litigation shall be provided continued protection. Information so provided, and information and materials required by a court to be introduced into evidence with appropriate protection, shall not be viewed as having been officially disclosed and will retain its classification status.

Section 2. Derivative Classification.

i. Proposal: Paragraph 2-302, which establishes declassification date marking requirements for various categories of classified information should be amended to conform with the revised declassification review procedures proposed in Section 3. (CIA).

Discussion: Paragraph 2-302 presently provides that derivative material is to be marked for declassification depending on the date of origin and type of information contained in the source material. New material deriving its classification from information classified under previous orders is to carry forward the original source material's declassification date if that date is twenty years or less from the source material's date of origin. If the source material bears no declassification date or is marked for declassification beyond twenty years, the derivative material is to be marked for declassification at a date not later than twenty years from the date of original classification of the source material. Foreign government information bearing no classification date or marked for declassification beyond thirty years must be marked for declassification review at a date no more that thirty years from

the source material's origin. Under changes proposed in Section 3, infra, a uniform thirty-year period would be established for systematic declassification review of all classified, and not merely foreign government, information. Paragraph 2-302's present twenty-year requirement should be amended to reflect this change. This provision of a uniform thirty-year review requirement removes any further need to separately provide for thirty-year declassification markings for foreign goverment information. Information which derives its classification from source material determined to be exempt from systematic declassification under revised section 3-4, infra, will not carry a declassification date, since exempted information under this new section is to be reviewed for declassification only at the request of a member of the public or another goverment agency.

Suggested Revision: 2-302. New material that derives its classification from information classified under prior Orders shall be treated as follows:

(a) If the source material bears a declassification date or event thirty years or less from the date of origin, that date or event shall be carried forward on the new material;

(b) If the source material bears no declassification date or event or is marked for declassification beyond thirty years, the new material shall be marked with a date for review for declassification at thirty years from the date of original classification of the source material;

(c) If the source material is information which is determined to be exempt from systematic declassification pursuant to section 3-4, the declassification review markings appied to the source material pursuant to section 3-4 shall be carried forward on the new material.

Section 3. Declassification and Downgrading.

Subsection 3-3. Declassification Policy.

i. Proposal: Paragraphs 3-301 and 3-302 should be reworded and Section 3-303 (balancing test) deleted altogether, to correct the present bias and overemphasis on declassification and release of national security information. (CIA, State, NSA, FBI, DOJ)

Discussion: Section 3-301's initial sentence requiring that declassification be "given an emphasis comparable to that accorded classification" should be deleted. The order's primary purpose is, and should remain, the protection of national security information. The remainder of this section is not objectionable, since it ties declassification to "national security considerations" and loss of the "information's sensitivity with the passage of time." Section 3-302 presently requires information to be declassified unless it is specifically found to continue to meet the classification requirements of Section 1-3. This section should be amended to reflect just the opposite emphasis, that is, that information may only be declassified if the classification requirements of Section 1-3 are found to no longer exist.

Paragraph 3-303 should be deleted in its entirety. That section directs agencies receiving FOIA or declassification requests to undertake a balancing test in certain cases to determine whether the "need to protect such information may be outweighed by the public interest in disclosure of the information," and in such cases where the public interest is

found to be weightier, agencies are directed to release such information under the FOIA or to declassify it. This balancing test has been viewed by certain requesters and courts as imposing a third component to the classification process: (a) information must fit within an enumerated category of classifiable information; (b) its disclosure must result in some harm to the national security; and (c) that harm must not be outweighed by the "public interest" in disclosure.

This balancing provision has come to play an increasing role in FOIA cases and has provided FOIA requesters and courts with a further basis for reviewing substantive agency determinations concerning classification and harm to the national security. Courts which may otherwise feel uncomfortable in making decisions which may impact on the national security, feel less constrained to examine the "public's interest" in such matters and are encouraged to do so by the ambiguous inclusion of this balancing test in the order's declassification section. Despite Executive Branch disavowals of any intent to alter the substantive requirements of classification through the provision of this balancing test in Section 3-303, requesters are increasingly asserting a mandatory right to judicial review of agency classification decisions under this provision.

The Congress, in fashioning the FOIA, specifically recognized that in cases involving these two competing governmental interests - increased public access to government information and protection of information essential to national

security - the latter interest will prevail. Implicit in the decision to classify information is a determination that the public interest in disclosure is outweighed by the public interest in safeguarding information necessary for the nation's defense and security. Once information is determined to be classifiable, and harm can reasonably be expected from its disclosure, generalized assertions of public interest raised under the FOIA by one person purporting to act for the public's benefit should not subject an otherwise valid classificaiton decision to further challenge by a requester or review by the courts.

> Suggested Revision: 3-301. Information classified pursuant to this and prior Orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or on the occurrence of a declassification event.
>
> 3-302. Information reviewed for declassification pursuant to this Order or the FOIA, may only be declassified if the declassification authority established pursuant to Section 3-1 determines that the information fails to meet the classifiation requirements prescribed in Section 1-3.

Subsection 3-4. Systematic Review for Declassification

i. Proposal: Classified information pertaining to intelligence sources, methods, or activities; cryptography; foreign government information; or information which disclosure would place an individual's life in immediate jeopardy should be exempted from systematic declassification review. After the passage of ten years, such "exempt" information would be

subject to review for declassification when a request for release of this information is received from a member of the public or another government agency. All other classified information not falling within one of the above categories would be systematically reviewed for declassification as it becomes thirty years old. Promulgation of guidelines for the systematic review of classified information would be continued, with expanded authority in this regard provided the DCI with respect to intelligence sources and methods information, and DOD with respect to cryptographic information. Review under these guidelines could be undertaken by category of documents, rather than on the present document-by-document basis. (CIA, State, NSA, FBI).

Discussion: Subsection 3-4 provides that information constituting permanently valuable records of the Government must be reviewed for systematic declassification at the end of 20 years, but classification may be extended for ten-year periods provided the information is reviewed at the end of each period. Foreign government information may be classified for a 30-year period. The Director of ISOO may extend this review period for specific categories of information. Subsection 3-5 also provides a mandatory review procedure, which requires agencies to conduct a review upon request to either the National Archives ("NARS") or the originating agency of requested documents and declassify and release those documents no longer requiring protection.

The present executive order exempts foreign government information from automatic and twenty-year systematic declassification review, but provides no similar provision for information relating to intelligence sources and methods and other classified information. The imposition a twenty-year systematic declassification review for intelligence sources and methods information, and a 30 year declassification review for foreign government information, fails to recognize the continuing need for protection of much of this intelligence and foreign government information beyond any artifically imposed time period. Moreover, it requires time-consuming and costly page-by-page review of information which frequently is of no interest to the public and which is never likely to be the subject of a FOIA or mandatory review request. A recent General Accounting Office Report, LCD-81-3, "Systematic Review for Declassification of National Security Informtion -- Do Benefits Exceed Costs?" (15 October 1980), recommended that E.O. 12065 be revised to limit systematic review to only those records requested by the public. This revision is particularly appropriate for cryptologic information, foreign government information, intelligence source, method, and activity information, and life-endangering information which requires a longer period of protection than that required for other categories of classified information.

The provisions of E.O. 11652 were much more practicable in recognizing both the administrative burden occasioned by

requiring systematic review of all classified information, and the public's right to have such a review implemented in cases of particular need. The present declassification section should be revised along the lines of section 5 of E.O. 11652, with the above categories of exemption provided for particularly sensitive classified information.

The above exemption categories are not meant to be exhaustive, but provide for exemption of categories of information falling into the primary areas of concern: foreign government, intelligence sources and methods and cryptographic information, and information whose disclosure could immediately endanger individual lives. E.O. 11652 also provided categories of exemption for information relating to material disclosing a "system, plan, installation, project, or specific foreign relations matter requiring continuing protection."

E.O. 11652 required an automatic declassification review of such exempted information to be conducted thirty years from the date of the information's origin. Several suggested revisions would subject foreign government and intelligence source information otherwise exempted from automatic and systematic declassification review to review for declassification after a certain time period (i.e., thirty or seventy-five years). Whether review is required after the passage of twenty, thirty, or seventy-five years, mandatorily requiring agencies to review information that has not been requested by the public is a time-consuming, administratively costly, and unnecessary burden

to impose upon an agency. Moreover, if foreign government information is required to be reviewed after thirty years, and intelligence source information after seventy-five years or some differing time period, foreign government information intermingled with intelligence source information in the same document would have to be identified and segregrated in order to comply with these differing review requirements. Rather than expending agency resources in this manner, a declassification review of exempted material should be conducted only after a request is received from a member of the public or another agency. Review procedures for foreign government information would be developed by agency heads in consultation with the Archivist. Similar guidelines promulgated by the DCI and the DOD would apply to the review of intelligence sources and methods information and cryptographic information, respectively, regardless of the location of the records or the agency having actual physical custody of this information. The promulgation of such guidelines by the DCI and DOD would require the deletion of the duplicative authority provided in Section 3-403 to establish guidelines for the systematic review and declassification of information concerning the identities of clandestine human agents and classified cryptographic information. Unlike the presently provided authority in Section 3-403, these DCI and DOD developed guidelines would not be subject to approval by ISOO, but would, like the foreign government guidelines authorized by paragraph 3-404, be available for use upon approval of the issuing agency.

Information which does not fit within any of the exemptions provided by the revised paragraph 3-403, would continue to be subject to systematic review for declassification pursuant to paragraphs 3-401 and 3-402. Unlike the present order, however, the initial period of review would be extended to thirty years and would apply uniformly to all classified information. Guidelines for systematic review of thirty year old classified information not otherwise exempted by Section 3-403 would be developed by agencies for information under their jurisdiction. These guidelines would specify those categories of information which should not be automatically declassified after thirty years, but which should be reviewed to determine the need for continued classification. Unlike the present order which requires such review to be undertaken on an item-by-item basis, the revised order would permit agency determinations as to the need for continued classification to be made by categories of documents. Establishing a uniform thirty year period for review, permitting review at that time to be undertaken by category rather than individual document, and exempting from such review information which can normally be expected to require protection beyond this thirty year period, should ease the administrative burdens of systematic declassification while continuing to make available that information requested by the public and other interested parties.

The thirty year declassification review procedures of paragraphs 3-401 and 3-402 and the exemption provision of 3-403,

will apply to information originated both before and after the effective date of the order. Information classified before the effective date of the order will be subject to systematic review after the passage of thirty years, at which time the information will either be declassified, its classification continued under the guidelines promulgated by agency heads pursuant to 3-402, or will be determined to be exempt from systematic declassification under section 3-403. As with information classified after the effective date of the order, previously classified information will also be subject to mandatory classification review upon request by members of the public or other agencies under the conditions provided by section 3-403 and 3-501. When so requested, information may be determined to be exempt under section 3-403 and thus subject to such review only after the passage of ten years, or if not so exempt or if more than ten years old, either declassified and released or its classification continued as required by the above provisions. The revisions suggested in Section 2-302 of the present order, which concern declassification marking requirements for new material whose classification derives from source material classified under previous orders, reflect the above transition scheme.

Suggested Revision: 3-4. Systematic Review for Declassification.

3-401. Classified information constituting permanently valuable records of the Government, as defined by 44 U.S.C. 2103, and information in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, whether originating before or after the

effective date of this order shall be reviewed for declassification as it becomes thirty years old.

3-402. Agency heads listed in Section 1-2 and the heads of agencies which had original classification authority under prior orders shall, after consultation with the Archivist of the United States and the Information Security Oversight Office, issue and maintain guidelines for systematic review covering thirty-year old classified information under their jurisdiction. These guidelines shall state categories of information which, because of their national security sensitivity, should not be declassified automatically but should be reviewed to determine whether continued protection beyond thirty years is needed. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information.

3-403. (a) Certain classified information may warrant protection for a period exceeding that provided in the automatic and systematic declassification provisions of sections 1-4 and 3-401. An official with Top Secret classification authority may exempt from the above automatic and 30-year systematic declassification provisions any level of classified information or material originated by him or under his supervision if it falls within one of the categories described below. In each case such official shall specify in writing on the material the exemption category being claimed. The use of the exemption authority shall be consistent with national security requirements and shall be restricted to the following categories:

(1) Foreign government information;

(2) Classified information specifically covered by statute, or disclosing intelligence activities, sources or methods, or pertaining to cryptography; and

(3) Classified information the disclosure of which would place a person's life in immediate jeopardy.

(b) All classified information and material originated either before or after the effective date of this order which is exempted under (a) above from automatic and systematic declassification shall be subject to a classification review by the originating agency at any time after the expiration of ten years from the date of origin provided:

(1) An agency or member of the public requests a review;

(2) The request describes the record with sufficient particularity to enable the agency to identify it; and

(3) The record can be located and obtained with a reasonable amount of effort. Information or material which no longer qualifies for exemption under (a) above shall be declassified. Information or material continuing to qualify under (a) shall be so marked. Review of foreign government information exempted under 3-404 (a)(1) and life-endangering information exempted under 3-404(a)(3), shall be in accordance with the provisions of Section 3-3 and with guidelines developed by agency heads in consultation with the Archivist of the United States and, where appropriate, with the foreign government or international organization concerned. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information. Review of intelligence source, method and activity information excepted under 3-404(a)(2) shall be in accordance with the provisions of Section 3-3 and with guidelines developed by the Director of Central Intelligence. Such guidelines will be used by the Archivist of the United States and any agency having custody of intelligence sources, methods or activities information. Review of classified cryptologic information exempted under 3-404(a)(2) shall be in accordance with special procedures established by the Secretary of Defense.

Subsection 3-5. Mandatory Review for Declassification.

i. Proposal: Minor technical amendments reflecting the changes effected in section 3-4 should be made in section 3-5. (CIA).

Discussion: Section 3-5 of the present order provides procedures for processing mandatory declassification requests received from members of the public or other government agencies or employees. These procedures are very similar to those provided by former section 5(c) of E.O. 11652 and require only minor technical changes to conform with the revised declassification provisions of section 3-4.

Suggested Revision: 3-501. Agencies shall establish a mandatory review procedure to handle requests by a member of the public, by a government employee, or by an agency, to declassify and release information. This procedure shall apply to information classified under this Order or prior Orders. Except as provided in Section 3-503, upon such a request the information shall be reviewed for possible declassification, provided the request satisfies the conditions provided by section 3-403(b). Requests for declassification under this provision shall be acted upon within 60 days. After review, the information or any reasonably segregable portion thereof that no longer requires protection under this Order shall be declassified and released unless withholding is otherwise warranted under applicable law.

3-503. Information less than ten years old which falls within the exemption categories provided by section 3-403 or which was originated by the President, by the White House Staff, or by committees or commissions appointed by the President, or by others acting on behalf of the President, including such information in the possession and control of the Administrator of General Services pursuant to 44 U.S.C. 2107 or 2107 note, is exempted from the provisions of Section 3-501. Such information when ten years old shall be subject to mandatory review for

declassification. Requests for mandatory review shall be processed in accordance with the provisions of section 3-403(b) and the guidelines promulgated thereunder.

ii. Proposal: Paragraph 3-505 should be amended to affirmatively authorize the use of [ ] responses in appropriate cases. (CIA, NSA). STAT

Discussion: Paragraph 3-505 provides that agencies receiving requests for information under either the above mandatory review procedures or the FOIA, may not refuse to confirm or deny the existence or nonexistence of documents unless the fact of their existence or nonexistence would itself be classifiable under the Order. The retention of this limitation on the [ ] response is desirable to avoid a growing tendency STAT to use this response indiscriminately to avoid burdensome processing or problems relating not to the existence of documents but to the underlying sensitivity of the information contained in such documents. Agencies' ability to defend such a response is dependent on its judicious use and the degree to which officials can clearly articulate and distinguish between the harm occasioned by acknowledging the existence or nonexistence of documents and the actual injury involved in releasing the information contained in the documents themselves. The present negative wording of paragraph 3-505 should be changed, however, to instead provide an affirmative authorization for such a response in appropriate cases. This section, as presently worded, has been interpreted by several courts as establishing a presumption against the use of such a nonconfirmation response.

Rebutting this presumption often results in disclosure or compromise of the fact that is sought to be protected. While this provision should thus be retained to limit nonconfirmation responses to cases of legitimate need, it should be reworded to provide positive authority for such a response when the circumstances so warrant.

> Suggested Revision: 3-505. An Agency in possession of classified information or material may, in response to a request for records under the Freedom of Information Act or this Order's Mandatory Review provision, refuse to confirm or deny the existence or non-existence of the information or material, when the fact of its existence or non-existence would itself be classifiable or would reveal an intelligence activity or source.

3-6. Downgrading.

i. Proposal: Paragraph 3-602 should be amended to provide that the downgrading of classified information may be effected only by the originator of that information or by officially authorized successors to the originator. (CIA).

Discussion: Paragraph 3-602 authorizes the downgrading of classified information by the information's "originator" or by "other authorized officials." While most agencies have viewed this provision as permitting a lower classification to be assigned only by the originator or an individual succeeding to the responsibilities of the originator (i.e., CIA for OSS), other agencies have interpreted this section to mean that any authorized recipient may downgrade material provided notice is given to the "holder of the information to the extent practicable." To clarify the intent of this provision and to

avoid any ambiguity in this regard, paragraph 3-602 should specifiy that such downgrading is to be effected only by the originator or by officially authorized successors to the originator.

> Suggested Revision: 3-602. Classified information that is not marked for automatic downgrading may be assigned a lower classification designation by the originator or by officially authorized successors to the originator when such downgrading is appropriate. Notice of downgrading shall be provided to holders of the information to the extent practicable.

3.7 Upgrading (New).

i. Proposal: A new section 3.7 dealing with the upgrading of classified information should be added to the order.

Discussion: The addition of this provision would achieve a better balance between the present order's emphasis on declassification and the need to adequately safeguard national security information. This section is modeled on section 4(g) of former E.O. 10501.

> Suggested Revision: 3.7. Upgrading. If the recipient of unclassified material believes that it should be classified, or if the recipient of classified material believes that its classification is not sufficiently protective, it shall be safeguarded in accordance with the classification deemed appropriate and a request made to the originator or the officially authorized successor to the originator, who may classify the material or upgrade the classification when such upgrading is appropriate.

Section 4. Safeguarding.

4.1. General Restrictions On Access.

i. Proposal: Greater specificity should be provided in Section 4-1 as to the minimum requirements that must be satisfied before access is provided to classified information. Additionally, the denial or revocation of an individual's clearance by one agency should preclude issuance of such a clearance by another agency unless the original denying agency, or the National Security Council ("NSC") on appeal, concurs in approving the renewed request for clearance. (CIA).

Discussion: Paragraph 4-101 presently provides that a person shall not be provided access to classified information unless that person is determined to be trustworthy and unless access is necessary for the performance of official duties. This section needs to be amplified to provide for the promulgation by agency heads of minimum security investigation standards that must be satisfied in such cases. Procedures for withdrawing previously granted clearances when no longer needed or required should also be adopted by agencies. Additionally, greater uniformity in such clearance determinations should be encouraged by requiring agencies that are considering individuals who have had an earlier clearance by another agency denied or revoked for security reasons to consult and obtain the approval of that denying agency prior to granting the clearance. If the original denying agency refuses to approve the granting of this clearance, this denial would be appealable to the National Security Council.

Suggested Revision: A person is eligible for access to classified information only after a favorable determination of trustworthiness has been reached by agency heads or designated senior officials based upon appropriate investigations in accordance with applicable standards and criteria, and provided that such access is essential to the accomplishment of official Government duties or contractual obligations. Agency heads listed in section 1-2 shall issue and maintain minimum security investigative standards that must be satisfied for each of the three national security information classification designations before access to such information is provided. Each agency shall make provision for administratively withdrawing the security clearance of any person who no longer requires access to classified information in connection with the performance of official duties, or if a person no longer requires access to a particular security classification category, the security clearance shall be adjusted to the classification category still required for the performance of official duties. An individual whose clearance has either been denied or revoked for security reasons by an agency, may not thereafter be granted access to classified information by another agency unless the approval of the initial denying agency is obtained. If the initial denying agency refuses to approve such access, this denial may be appealed to the National Security Council. The denial of access shall remain in effect until the appeal is decided.

This will be deleted, per STAT STAT

6 May 81

STAT

4-2. Special Access Programs.

i. Proposal: Paragraph 4-201 should be amended to provide that the DCI is to establish uniform security standards to govern access to, distribution of, and protection of information relating to intelligence sources and methods. (CIA).

Discussion: Subsection 4-2 authorizes agency heads with original classification authority to create special access programs in order to control the access and distribution of particularly sensitive information. The DCI is provided with the sole authority to create and continue special access programs and

compartmentation controls with respect to matters pertaining to intelligence sources and mehtods. The authority provided the DCI in this section should be expanded in order to promote uniformity of standards within constraints set by cost and security needs.

> Suggested Revision: Agency heads listed in Section 1-201 may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or prior Orders. Such programs may be created or continued only by written direction of the above agency heads. For special access programs pertaining to intelligence sources and methods, this function will be exercised by the Director of Central Intelligence, who will prescribe security, access, and control standards for such programs.

ii. Proposal: Paragraph 4-202's requirement that the use of special access programs be limited to circumstances in which the number of persons requiring access will be "reasonably small" should be revised to more accurately reflect the real concern of confining access to persons with a real need to know. (CIA).

Discussion: Paragraph 4-202 sets forth certain criteria which special access programs must satisfy to be created or continued. The second requirement that "the number of persons who will need access will be reasonably small" provides little useful guidance in determining whether the creation of a special access program is appropriate. This requirement should be amended to better reflect its real concern of restricting access to that bare minimum who require access because of a real need to use this information.

Suggested Revision: 4-202 (b) The number of persons provided access will be maintained at a minimum commensurate with the objective of providing extra protection for the information involved.

iii. Proposal: Paragraph 4-204, which provides for special access program accounting procedures, should be amended to conform with the expanded authority provided the DCI under §4-202 to promulgate guidelines with respect to intelligence source and method special access programs.

4-204. Suggested Revision: ...Each of those agency heads, and for intelligence source and method related special access programs, the Director of Central Intelligence, shall also establish and maintain a system of accounting for special access programs.

4.3. Access by Historical Researchers and Former Presidential Appointees.

i. Proposal: The present exemption provided historical researchers and former Presidential appointees from the requirement of paragraph 4-101, that access to classified information be granted only for the performance of official duties, should be continued but this access should be subject to more rigorous safeguards on such persons' further use of this information. (CIA).

Discussion: Access is presently provided to historical researchers and Presidential appointees only after a written determination that access is consistent with the interests of national security. This requirement does not sufficiently safeguard classified information in all cases. Further provisions conditioning access on: (a) the researcher's agreement

to safeguard the information in a manner consistent with the order; and (b) the researcher's authorization of a review of his notes and manuscript for the sole purpose of determining that no classified information or material is contained therein should be available for use at an agency's option in certain cases.

Suggested Revision: 4-303. (New)
Persons granted waivers under Section 4-301 may be required, in appropriate cases, to enter into a written agreement authorizing agency review of the individual's notes and manuscript to ensure that no classified information is contained therein, and requiring individuals to safeguard such information in a manner consistent with this order.

4-4. Reproduction Controls.

i. Proposal: Greater flexibility should be authorized in the permissible range of restrictions which may be imposed on the reproduction and dissemination of classified materials. (CIA, NSA).

Discussion: Paragraph 4-401 prohibits the reproduction of Top Secret material without the consent of the originating agency. The mandatory limitations on reproduction of Top Secret material should be eased, and reproduction and dissemination controls imposed as determined to be needed by the originator for all levels of classified information. Paragraph 4-401 and 402 should be combined in this regard to permit such flexible controls to be utilized with regard to all levels of classified information.

Suggested Revision: 4-401.
Reproduction or dissemination of classified documents may be prohibited or restricted by the originator.

ii. Proposal: Paragraph 4-404 should be amended to delete the present inventorying requirements imposed on documents covered by special access programs. (CIA, NSA).

Discussion: The cost of implementing inventorying controls for special access program information would be prohibitive and would produce no measurable improvement in security. Inventorying controls and standards for special access program materials should instead be prescribed under the authority provided agency heads to establish special access programs under paragraph 4-201.

> Suggested Revision: 4-404. Records shall be maintained by all agencies that reproduce paper copies of classified documents to show the number and distribution of reproduced copies of all Top Secret documents, and of all Secret and Confidential documents which are marked with special dissemination and reproduction limitations in accordance with section 1-506 and 4-401. Procedures governing the reproduction and inventorying of documents covered by special access programs shall be prescribed by agency heads pursuant to the authority provided by section 4-201.

iii. Proposal: Paragraph 4-405 should be amended to make clear that documents reproduced for the purpose of facilitating declassification reviews are to be destroyed after this determination has been made. (CIA).

Discussion: The present language of paragraph 4-405 requiring the destruction of documents "after they are used," does not clearly delineate the "use" to which it is referring. This paragraph should be amended to remove any ambiguity in this regard by clearly stating that destruction is to occur after the declassification review has been completed.

Suggested Revision: 4-405. Section 4-401 shall not restrict the reproduction of documents for the purpose of facilitating review for declassification. However, such reproduced documents that remain classified after review must be destroyed after such a determination has been made.

iv. Proposal: A new paragraph 4-406 should be added which would directly incorporate in the EO the "third agency rule" presently provided at ISOO Directive No. 1, Section IV D. (CIA).

Discussion: The "third agency" rule makes clear that classified information is not to be disseminated without first obtaining the consent of the originating agency. Its inclusion in the order would ensure that the originating agency's equities are directly considered before such information is released.

Suggested Revision: 4-406 (New). Except as otherwise provided by section 102 of the National Security Act of 1947, 61 Stat. 495, 50 U.S.C. 403, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency.

Section 5. Implementation and Review.

Subsection 5-4. General Responsibilities.

i. Proposal: Substantive classification guides should be required to be promulgated by agencies only when their development and use is practicable and will further the administration of the order. (State, FBI).

Discussion: Paragraph 5-403 requires agencies with original classification authority to promulgate guidelines to facilitate the identification and uniform classification of information under the order. Several agencies have noted the

impossibility of developing useful substantive classification guides in the foreign affairs and intelligence source and method areas. Rather than mandatorily requiring the development of such guidelines, their provision should be limited to circumstances in which their development and use is both practicable and beneficial.

Suggested Revision: 5-403. Agencies with original classification authority shall, whenever useful, promulgate guides for security classification...

ii. Proposal: Paragraph 5-404, which delineates an agency's general responsibilities in implementing the order, should be revised to reflect a more appropriate balance between the declassification and safeguarding of information. Paragraph 5-404(d)'s encouragement of challenges to agency classification decisions should be revised, and present paragraph 5-404(g) should be deleted and replaced by a new paragraph establishing active training and orientation programs for employees responsible for safeguarding classified information. (State, CIA).

Discussion: Firstly, the last sentence of paragraph 5-404(d), which "encourages" agency personnel to challenge classification decisions, should be deleted. Appropriate procedures, including the mandatory review process, are available to agency personnel in this regard, removing any need to affirmatively exhort individuals to challenge classification determinations. Section 5-404(g), which provides for the systematic review and elimination of unnecessary agency safeguard

procedures, should be deleted. Instead, a new subsection (g) should be added to provide for the orientation and continuing education of agency employees involved in the safeguarding of classified information.

Suggested Revision: 5-404(g) (New).
To promote the basic purposes of this Order, agency heads shall designate experienced persons to maintain active training and orientation programs for employees concerned with classified information to impress upon such employees their individual responsibility for exercising appropriate care in safeguarding information in compliance with the provisions of this Order. Such persons shall be authorized on behalf of agency heads to establish adequate and active inspection programs to the end that the provisions of this Order are administered effectively.

Subsection 5-5. Administrative Sanctions.

i. Proposal: "Unauthorized disclosure" should be defined for purposes of imposing various criminal and administrative sanctions as including oral communications as well as physical transfers of classified information. (CIA).

Discussion: Paragraphs 5-502 and 5-503 provide that any knowing or negligent unauthorized disclosure of classified information may subject an individual to appropriate administrative and criminal sanctions. The varying degree of severity of the various administrative sanctions provided makes the imposition of such sanctions appropriate for negligent as well as deliberate unauthorized disclsoure of classified information. No definition of "unauthorized disclosure" is presently provided by this section. To make clear that this section is not limited to actual transfers of physical copies of

documents, "unauthorized disclosure" should be defined as either a communication or physical transfer of information or material to an unauthorized person. Additionally, the order of section 5-502(a) and (b) should be inverted, to emphasis the greater concern placed on unauthorized disclosure as opposed to wrongful classification of national security information.

> Suggested Revision: 5-502. Officers and employees of the United States Government shall be subject to appropriate administrative sanctions if they:
>
> (a) knowingly, willfully and without authorization disclose information properly classified under this Order or prior Orders or compromise properly classified information through negligence; or
>
> (b) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or
>
> (c) knowingly and willfully violate any other provision of this Order or implementing directive. Unauthorized disclosure for purposes of this section includes either a communication or physical transfer of classified information to an unauthorized person.

ii. Proposal: The reporting required by paragraph 5-505 of possible violations of federal criminal law should be undertaken in accordance with the reporting procedures provided for similar violations by E.O. 12036 and its implementing guidelines. (CIA).

Discussion: Paragraph 5-505 presently provides for prompt reporting of possible violations of Federal criminal law to the Attorney General and provides for the imposition of criminal sanctions for such violations. Paragraph 5-505 should

be amended to clarify the relation between the similar reporting requirements of E.O. 12065 and 12036. E.O. 12036 requires an agency to report possible violations of Federal criminal law committed by federal employees or other persons to the Department of Justice in accordance with guidelines developed by the Attorney General. E.O. 12065 requires similar reporting with respect to possible violations reflected in classified information or documents. E.O. 12065 should make clear that such violations are to be reported in conformity with the reporting procedures provided by E.O. 12036 and its implementing guidelines and that it does not otherwise intend to supersede or affect the reporting requirements of that order.

> Suggested Revision: 5-505. Agency heads shall report to the Attorney General evidence reflected in classified information of possible violations of Federal criminal law by an agency employee and of possible violations by any other person of those Federal criminal laws. Reporting of possible violations will be done in conformity with the reporting procedures promulgated by the Attorney General under the authority of 28 U.S.C. §535 and E.O. 12036, §§1-706 and 3-305. Nothing in this Order is intended to affect or otherwise supersede the reporting requirements provided in E.O. 12036 or the Attorney General guidelines implementing that order.

Section 6. General Provisions.

6-1. Definitions.

i. Proposal: The present definition of "foreign government information" should be amended to clearly provide that information, regardless of whether it would be considered classified if received from other sources, if received from a foreign government with the expectation, either expressed or

implied, that it will be held in confidence, will qualify as "foreign government information." Additionally, the requirement that information to qualify as "foreign government information" must be provided to the United States pursuant to a written agreement should be amended to remove the need for such arrangements to be evidenced by some type of written instrument. (Treasury, CIA, FBI).

Discussion: Paragraph 6-103 presently defines "foreign government information" as:

> "information that has been provided to the United States in confidence by, or produced by the United States pursuant to a written joint arrangement requiring confidentiality with, a foreign government or international organization of governments."

Certain foreign governments which are willing to enter into some sort of mutual cooperative arrangement are unwilling or reluctant to enter into a formal written agreement that evidences a relationship with a United States intelligence agency. The requirement that such agreements or arrangements be in writing inhibits the utility and availability of certain cooperative relationships. The word "written" should thus be deleted from the above definition of "foreign government information." Additionally, information provided the United States by foreign goverments with the expressed or implied understanding that it is to be held in confidence should be afforded this same protection. Even if this information might not be classified if originated by the United States, it is the expectation of confidentiality and the need to honor that commitment rather than

the actual sensitivity of the information itself that requires protection.

Suggested Revision: 6-103. Foreign goverment information means:

(a) Documents or material provided by a foreign government or governments, an international organization of governments, or any element thereof in the expectation, expressed or implied, that the document, material, or the information contained therein is to be held in confidence;

(b) Documents originated by the United States that contain classified information provided, in any manner, to the United States by foreign governments, international organizations of governments, or elements thereof, with the expectation, expressed or implied, that the information will be held in confidence;

(c) Classified information or material produced by the United States pursuant to or as a result of a joint arrangement, with a foreign government or organization of governments requiring that the information, the arrangement, or both be held in confidence.

ii. Proposal: A new paragraph 6-106 should be added to the revised order which would provide a definition of "confidential source" in accordance with the presumption of harm accorded to such sources by section 1-303. (State).

Discussion: The term "Foreign confidential source," as used in section 1-303 of the present order, unnecessarily limits the extent of protection afforded by that section's presumption of harm. U.S. citizens furnishing the Government with confidential information outside the United States or any person providing information to the Government inside the United States

would not be included within this language. Foreign newsmen providing information to an agency within the United States or U.S. businessmen furnishing information to a U.S. embassy abroad, for example, would not be entitled to the additional protection afforded by section 1-303. The modifier "foreign" should be deleted from confidential source as used in section 1-303, and a definition of "confidential source" should be included in a new section 6-106 which clearly emphasizes that the act of providing confidential information to the U.S. Government, and not the nationality or geographical location of the source, triggers protection under the order.

Suggested Revision: 6-106 (New). "Confidential source" means the identity of any individual who has provided, or may provide, classifiable information to the United States.